Keywords for Today’s lesson

What do the following words mean? Relate them digital devices and give examples where possible

1. **Threat**
2. **Purporting**
3. **Malicious**
4. **Exploit**
5. **Reputable**
6. **Bounty**

Keywords for Today's lesson

What do the following words mean? Relate them digital devices and give examples where possible

1. **Threat –** a person or thing likely to cause damage or danger
2. **Purporting –** appear to be or do something, especially falsely
3. **Malicious –** intending or intended to do harm.
4. **Exploit** - make use of (a situation) in a way considered unfair or underhand.
5. **Reputable –** someone or something(company) that is trustworthy or respectable
6. **Bounty –** a reward offered in an official way for the capture of someone or something.

Threats to Data, Information & Systems

TOPIC D – PROTECTING DATA AND INFORMATION

UNIT 1 – INFORMATION TECHNOLOGY SYSTEMS

FARHAN MUKADAM

Threats to Data, Information & Security

A business’ data, information and systems are extremely important

Using IT systems there are many things that can cause harm to your data, information and systems.

Can be malicious or complete accidents

Types of Threats

Malware

Hackers

Phishing

Accidental Damage

MalWare

Designed to harm or gain unauthorised access to a computer system.

Viruses – a program that copies and inserts itself into programs running on your computer system. Attaches itself.

- **Worms** – very similar to viruses, key difference do not need to attach themselves instead exploits security holes in systems to gain access.

- **Trojans** – a harmful program that masquerades as a legitimate software application. It doesn't self-replicate like worms and viruses.

- **Spyware** –monitors user activity for the purpose of stealing personal information.

Mozzerella
Firefox
Attention!
Your browser is out of date, some of extensions may interfere your work!
Please choose requiered update:
Firefox 16.1 SP1
Firefox 16.1 SP2
Firefox 16.1 SP2 + Antivirus protection (recommended)
Current version of your browser is out of date (16.0)
Install

Hackers

A hacker is someone who gains unauthorised access to a computer system.

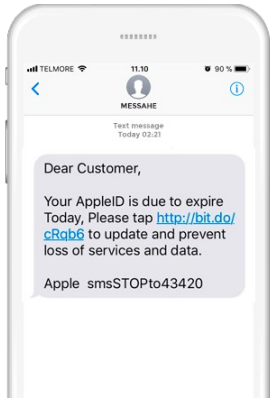
Simple as guessing someone’s password

Use programs that will automatically go through a list of common passwords

Not all hacking is malicious though.

“White hat hackers” test systems for security flaws

“Bounties” paid out to hackers who detect security flaws



HMRCUK
Sat 7 Apr, 13:29
You have a pending Tax Refund of 265.84GBP from HMRC. To proceed your application please complete your form via hmrc.gov.signin-uk.com

used Dropbox to share a file with you
Dropbox
I used Dropbox to share a file with you
For security purposes, you would be required to sign into your email address to view.
Click here to view.
© 2016 DropBox Inc.

Phishing

This is where emails are sent purporting to be a reputable company

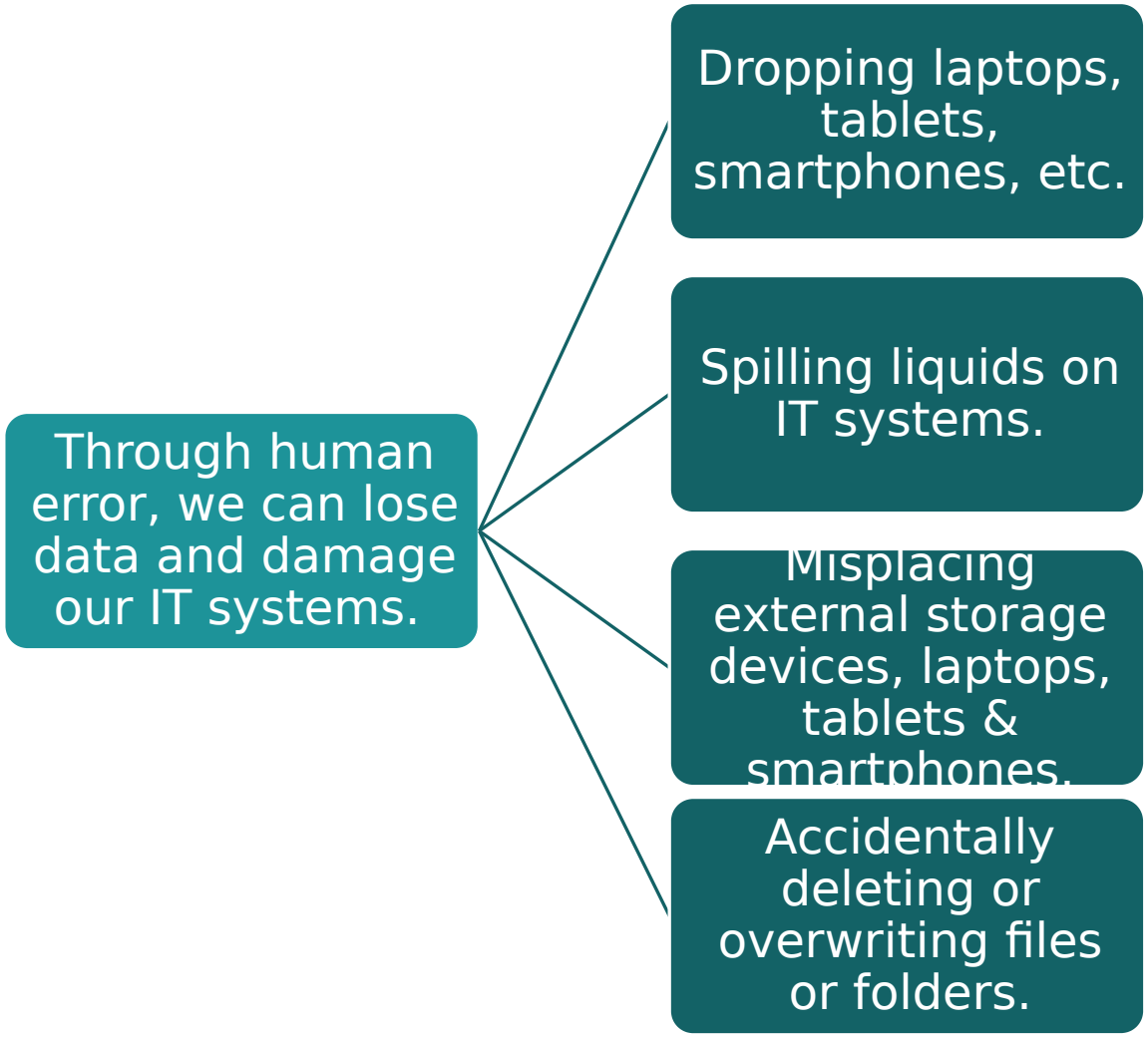
But have been sent by a malicious user for the purpose of gaining personal or financial information.

The email will appear to be from the reputable business

Contains a link that appears to be for their website.

Now seen phone phishing attempts

Accidental Damage


Through human error, we can lose data and damage our IT systems.
Dropping laptops, tablets, smartphones, etc.
Spilling liquids on IT systems.
Misplacing external storage devices, laptops, tablets & smartphones.
Accidentally deleting or overwriting files or folders.

Notes Activity – 20 mins

1. Look through additional slides in the PowerPoint on Threats to Data, information & Systems

2. Add **additional** notes for each Threat **- 2 Bullet Points minimum**

3. Add **Impact on Business** to your notes – What impact does each threat have on a business?

4. Add **Impact on Individual** to your notes – What impact does each threat have on a business?

Threats to Data, Information & Security

A business’ data, information and systems are extremely important to any organisation. They’re also extremely important to individuals who keep a lot of personal information on their computer systems that could cause great harm if lost or stolen.

Unfortunately, when using IT systems there are many things that can cause harm to your data, information and systems. These are often malicious users trying to steal data and purposely cause harm, but can also happen completely accidentally.

MalWare

computer program that is designed to harm or gain unauthorised access to a computer system. We most commonly are aware of viruses, and often use the term virus interchangeably with malware. However, viruses are just one type of

The key characteristics that define the different types of malware are:

Viruses – a program that copies and inserts itself into programs running on your computer system. It spreads when the programs or data files it is attached to are passed to another system, such as via an email attachment or files on a USB stick

Worms – very similar to viruses in many ways, the key difference is worms do not need to attach themselves to other programs. They instead are standalone programs and spread through tunnelling through a network and exploiting security holes in systems to gain access

Trojans – a harmful program that masquerades as a legitimate software application. It spreads by users downloading it thinking it is a program they want, but it hides a harmful payload. It doesn't self-replicate like worms and viruses.

Spyware – a malicious program that monitors user activity for the purpose of stealing personal information. An example would be a keylogger that records every keystroke a user makes and sends it back to a malicious user. This is commonly spread as part of a Trojan

Malware - Impacts on Individuals & Businesses

Malware can be used to corrupt or delete data being stored on IT systems. This could cause a lot of inconvenience to an organisation as they will need to spend time recovering the data from backups. If they have no backups then this could be disastrous as they could lose sales records, stock levels, employee pay data, etc.

The impact on individuals could be just as harmful. For example, personal photos that have real emotion value could be lost forever causing a lot of distress. Malware, especially spyware, could also be used to gather personal data, such as bank details, in order to steal money from individuals or to commit identity fraud.

Malware - Activity

There are many news stories where businesses have been impacted by malware.

Research these online and the consequences to the business.

Hackers

A hacker is someone who gains unauthorised access to a computer system. This can be performed in many ways, and not all are extremely technical. For example, guessing someone's password and using it to gain access to their computer system without their permission is hacking.

Hackers also use programs that will automatically go through a list of common passwords until it breaks into the computer system by eventually guessing the correct password. This is known as a "brute force attack". This type of attack is why we're encouraged to use complex passwords.

There are many other more technical methods of hacking which require programming knowledge and an understanding of the flaws in a computer system and its software.

Not all hacking is malicious though. So-called "white hat hackers" test systems for security flaws by attempting to gain access to help check the security procedures of an organisation. There are even "bounties" paid out to hackers who detect security flaws in software and report them to the organisation who developed the software.

Hackers - Impacts on Individuals & Businesses

Malware can be used to corrupt or delete data being stored on IT systems. This could cause a lot of inconvenience to an organisation as they will need to spend time recovering the data from backups. If they have no backups then this could be disastrous as they could lose sales records, stock levels, employee pay data, etc.

The impact on individuals could be just as harmful. For example, personal photos that have real emotion value could be lost forever causing a lot of distress. Malware, especially spyware, could also be used to gather personal data, such as bank details, in order to steal money from individuals or to commit identity fraud.

Hackers - Activity

Businesses, when they have been hacked, can often be fined under the Data Protection Act.

Research news stories where this has impacted on an organisation.

Phishing

This is where emails are sent purporting to be a reputable company but in fact have been sent by a malicious user for the purpose of gaining personal or financial information.

The email will appear to be from the reputable business and will usually contain a link that appears to be for their website. However, when clicked on it will take the user to another website that is designed to look like the business' but is not. This website will contain a form to be filled out with personal data and when submitted will go to the malicious user.

Most people don't fall for these threats but the malicious user can send the email to hundreds of thousands of users at no cost and so any user who makes the mistake will earn the malicious user profit.

Recently we've also seen phone phishing attempts, where people phone users claiming to be from a legitimate business to try and gain personal and financial information.

Phishing- Impacts on Individuals & Businesses

The goal of phishing is usually to obtain personal and financial information. This is therefore commonly used for stealing money from an individuals or an organisations bank account. Individuals can also be impacted by identity fraud, where personal data is stolen and used to sign up for loans for example.

The data stolen from organisations through a phishing email could be used to then perform a hack on the organisation. For example, a user may reveal their login details.

Phishing - Activity

A common version of phishing is an email pretending to be your bank and asking for you to enter your bank details.

How can you tell if an email is actually from your bank or not?

Accidental Damage

Not all damage to an IT system is malicious. Through human error, we can lose data and damage our IT systems. Some examples of this include:

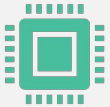
- Dropping laptops, tablets, smartphones, etc.
- Spilling liquids on IT systems.
- Misplacing external storage devices, laptops, tablets & smartphones.
- Accidentally deleting or overwriting files or folders.

All of these are done with no malicious intent but can have catastrophic consequences to the business as you could lose a massive amount of data. This is a major reason why businesses will perform regular backups to their data.

Accidental Damage- Impacts on Individuals & Businesses

Individuals may lose data, such as photos, with emotional value. Organisations may lose important business data such as sales records.

This is extremely expensive to recover from for both individuals and businesses. You may need to pay a specialist to try and recover the data or will need to recapture and re-enter data from its source.



Finally, you will need to replace any lost or damaged devices which will be costly too, especially to individuals.

Accidental - Activity

There have been cases where employees have left devices on trains or buses and the data has been stolen as a result.

Research online for any examples of this happening.

Threats to Data, Information & Security - Summary

Malware includes things like viruses, worms, trojans and spyware. This can corrupt or delete data which will be expensive to recover and can lead to data being stolen for bank fraud purposes.

Hackers are someone who gains unauthorised access to a computer system. Malicious hackers do so to misuse data, such as delete it, alter it or steal it for blackmail, bank fraud and identity fraud.

Phishing is where emails are sent purporting to be a reputable company, but in fact, has been sent by a malicious user for the purpose of gaining personal or financial information in order to commit bank or identity fraud.

Accidental damage is where IT systems or data are harmed through human error, such as dropping a device or accidentally overwriting important files. This can be costly, as you need to recover or re-enter the data that has been lost and replace harmed equipment.